ESET MOBILE SECURITY

POUR ANDROID

Manuel d'installation et guide de l'utilisateur

Cliquez ici pour télécharger la dernière version de ce document.

Sommaire

1. Installation d'ESET Mobile Security 3
1.1 Installation 3
1.2 Désinstallation 3
2. Activation du produit 4
3. Antivirus 4
4. Antispam 7
5. Anti-vol 8
6. Audit de sécurité 9
7. Mise à jour 10
8. Mot de passe 10
9. Dépannage et assistance 11
9.1 Dépannage 11
9.2 Assistance technique 11

ESET **MOBILE SECURITY**

Copyright ©2012 ESET, spol. s r.o.
ESET Mobile Security a été développé par ESET, spol. s r.o.
Pour plus d'informations, visitez www.eset.com/fr.
Tous droits réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système d'archivage ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement, numérisation ou autre, sans l'autorisation écrite de l'auteur.
ESET, spol. s r.o. se réserve le droit de modifier les applications décrites sans préavis.

Service client : http://support.athena-gs.fr/demande_de_support.php?editeur=eset

Rév. 25. 4. 2012

1. Installation d'ESET Mobile Security

Pour que vous puissiez installer ESET Mobile Security pour Android, votre appareil mobile doit disposer de la configuration système suivante :

	Configuration système minimum
Système d'exploitation	Android 2.0/2.1 (Éclair) et version ultérieure
CPU	600 MHz
RAM	256 Mo
Espace disponible dans la zone de stockage interne	5 Mo

REMARQUE : certaines fonctionnalités telles que Antispam et Anti-Theft ne sont pas disponibles sur les tablettes/ Android 3.0 ne prenant pas en charge les appels et la messagerie. Vous trouverez plus de détails dans cet article de la base de connaissances (peut ne pas être disponible dans votre langue).

1.1 Installation

Pour installer ESET Mobile Security, effectuez l'une des opérations suivantes :

- recherchez ESET Mobile Security (ou simplement Eset) dans l'application Google Play Store sur votre appareil Android. ESET Mobile Security est répertoriée dans **Applications** > **Outils**. Vous pouvez également installer le programme en numérisant le code QR à l'aide de votre appareil mobile et d'une application comme QR Droid ou Barcode Scanner.

- téléchargez le fichier d'installation de ESET Mobile Security *(ems.apk)* depuis le site Internet d'ESET en numérisant le code QR ci-dessous.

- téléchargez le fichier *ems.apk* sur votre ordinateur depuis le site Internet d'ESET. Copiez le fichier sur votre appareil par Bluetooth ou USB. Appuyez sur l'icône de lancement dans l'écran d'accueil Android (ou sélectionnez **Accueil** > **Menu**) et sur **Paramètres** > **Applications** et assurez-vous que l'option **Sources inconnues** est sélectionnée. Recherchez le fichier *ems.apk* à l'aide d'une application du type ASTRO File Manager ou ES File Explorer. Ouvrez le fichier et appuyez sur **Installer**. Une fois l'application installée, appuyez sur **Ouvrir**.

Avertissement : ESET Mobile Security doit être installé sur le stockage interne de l'appareil. Certains téléphones mobiles autorisent par erreur les utilisateurs à installer des applications sur la carte SD. Si vous installez ESET Mobile Security sur une carte SD, les fonctions Protection en temps réel, Antispam et Anti-vol ne fonctionneront pas.

Une fois ESET Mobile Security installé, vous devez l'activer en suivant les étapes de la section Activation du produit 4.

1.2 Désinstallation

Si vous souhaitez désinstaller ESET Mobile Security de votre appareil mobile, utilisez l'option **Assistant de désinstallation** accessible depuis l'écran principal d'ESET Mobile Security ou effectuez les opérations ci-dessous :

1. Appuyez sur l'icône de lancement dans l'écran d'accueil Android (ou sélectionnez **Accueil** > **Menu**). Appuyez ensuite sur **Paramètres** > **Localisation et sécurité** > **Administrateurs**, désélectionnez **ESET Security** et appuyez sur **Désactiver**. Entrez votre mot de passe ESET Mobile Security lorsque le système vous le demande. (Si vous n'avez pas défini ESET Mobile Security en tant qu'administrateur de l'appareil, ignorez cette étape.)
2. Revenez à **Paramètres** et appuyez sur **Applications** > **Gérer applications** > **ESET Security** > **Désinstaller** .

ESET Mobile Security et le dossier de quarantaine sont supprimés de manière permanente de votre appareil mobile.

2. Activation du produit

Après son installation, ESET Mobile Security doit être activé. Appuyez sur **Activer maintenant** dans la fenêtre principale d'ESET Mobile Security.

Les méthodes d'activation varient selon que vous avez téléchargé ESET Mobile Security depuis le site Internet d'ESET ou depuis Google Play.

- **Activer la version d'essai** - Sélectionnez cette option si vous ne disposez pas de licence et souhaitez évaluer ESET Mobile Security avant d'en faire l'acquisition. Indiquez votre **adresse électronique** pour activer ESET Mobile Security pendant une période limitée. Vous recevrez un message de confirmation vous informant du succès de l'activation du produit. La licence de test ne peut être activée qu'une seule fois par appareil mobile.
- **Activer à l'aide d'une clé d'activation** - (cette option n'est pas disponible si vous avez installé ESET Mobile Security depuis Google Play) si vous avez fait l'acquisition du programme avec un nouvel appareil (ou dans un boîtier), vous avez reçu une clé d'activation au moment de l'achat. Saisissez les informations que vous avez reçues dans le champ **Clé d'activation**, ainsi que votre adresse dans le champ **Email**. Les nouvelles données d'authentification (Nom d'utilisateur et Mot de passe) remplaceront automatiquement la clé d'activation et seront envoyées à l'adresse électronique que vous avez indiquée.
- **Activer à l'aide d'un nom d'utilisateur et d'un mot de passe** - (cette option n'est pas disponible si vous avez installé ESET Mobile Security depuis Google Play) si vous avez acheté votre produit auprès d'un revendeur, vous avez reçu un nom d'utilisateur et un mot de passe au moment de l'achat. Entrez ensuite les informations que vous avez reçues dans les champs **Nom d'utilisateur** et **Mot de passe**. Saisissez votre adresse dans le champ **Email**.
- **Renouveler la licence** - sélectionnez cette option si votre licence actuelle est sur le point d'expirer. Entrez vos **Nom d'utilisateur** et **Mot de passe** (données fournies au moment de l'achat de la licence actuelle) dans les champs appropriés.
- **Charger les données de licence** - (cette option n'est pas disponible si vous avez téléchargé ESET Mobile Security depuis le site Internet d'ESET) utilisez cette option si vous avez déjà acheté le programme avec ce compte. ESET Mobile Security sera activé en chargeant vos données de licence depuis le serveur ESET.
- **Acheter maintenant** - Sélectionnez cette option si vous n'avez pas de licence et souhaitez en acheter une.

Chaque activation n'est valide que pour une durée déterminée. Une fois l'activation expirée, vous serez invité à renouveler la licence du programme (le programme vous en avertira à l'avance).

REMARQUE : pendant l'activation, l'appareil doit être connecté à Internet. Des données seront téléchargées.

Par défaut, ESET Mobile Security est installé dans la langue qui est définie dans les paramètres régionaux de votre téléphone (dans les paramètres de langue et de clavier). Si vous souhaitez changer la langue de l'ensemble de l'interface utilisateur de l'application, sélectionnez **Langue** dans l'écran principal de ESET Mobile Security et sélectionnez la langue de votre choix.

3. Antivirus

Analyser l'appareil

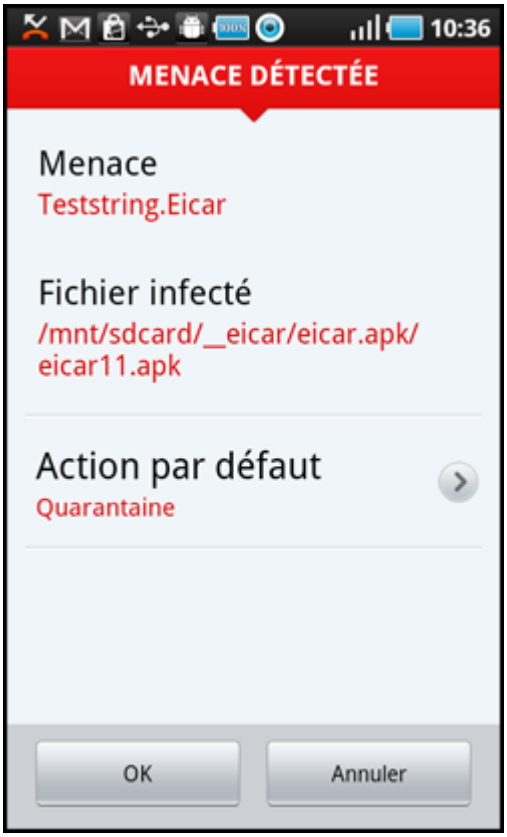
L'option **Analyser l'appareil** permet de rechercher la présence éventuelle d'infiltrations sur votre appareil mobile.

Certains types de fichiers prédéfinis sont analysés par défaut. Une analyse complète de l'appareil vérifie la mémoire, les processus en cours, les DLL (bibliothèques de liaison dynamiques) qui en dépendent, ainsi que les fichiers faisant partie de la zone de stockage interne et des supports amovibles. Une fois l'analyse terminée, un récapitulatif des résultats apparaît : nombre de fichiers infectés, nombre de fichiers analysés, durée de l'analyse, etc.).

Si vous souhaitez interrompre une analyse en cours, appuyez sur **Annuler**.

Analyser le dossier

Pour analyser certains dossiers de votre appareil, appuyez sur **Analyser le dossier**. Recherchez les dossiers à analyser, cochez les cases correspondantes dans la colonne de droite et appuyez sur **Analyse**.



Menace détectée par ESET Mobile Security

Journaux d'analyse

La section **Journaux d'analyse** contient des journaux qui fournissent des informations complètes sur les tâches d'analyse réalisées. Les journaux sont créés à chaque analyse déclenchée manuellement (à la demande) ou lorsqu'une infiltration a été détectée par l'analyse en temps réel.

Chaque journal contient les éléments suivants :

- la date et l'heure de l'événement ;
- le nombre de fichiers analysés ;
- le nombre de fichiers infectés ;
- le nom et le chemin d'accès complet des fichiers infectés ;
- la durée de l'analyse ;
- les actions exécutées ou les erreurs rencontrées lors de l'analyse.

Quarantaine

La principale fonction de la quarantaine consiste à stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer, ou encore s'ils sont détectés à tort par ESET Mobile Security.

Les fichiers stockés en quarantaine peuvent être affichés dans un journal qui indique le nom et l'emplacement d'origine des fichiers infectés, ainsi que la date et l'heure de leur mise en quarantaine.

Si vous souhaitez restaurer un fichier mis en quarantaine dans son emplacement d'origine, appuyez sur le fichier et sélectionnez **Restaurer**. Cette option n'est pas recommandée.

Pour supprimer de manière permanente un fichier mis en quarantaine de votre appareil, appuyez sur le fichier et sélectionnez **Supprimer**. Pour supprimer tous les fichiers stockés dans la quarantaine, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

Paramètres

Les paramètres **À la demande** permettent de modifier les paramètres d'analyse à la demande (déclenchée manuellement).

L'option **Boîte de dialogue Afficher les alertes** affiche des notifications d'alerte chaque fois qu'une nouvelle menace est détectée par l'analyse à la demande.

Si vous souhaitez analyser toutes les applications (fichiers *.apk*) installées sur l'appareil, sélectionnez l'option **Analyser les applications**.

La **protection proactive** est une méthode de détection basée sur un algorithme, qui analyse le code et recherche tout comportement typique de virus. Elle permet notamment d'identifier les logiciels malveillants qui ne sont pas encore identifiés par la version actuelle de la base des signatures de virus. Si la protection proactive est activée, l'analyse est plus longue.

L'option **Profondeur d'analyse des archives** permet d'indiquer le nombre de niveaux d'imbrication des archives (fichiers *.zip*) à analyser. Plus le nombre est élevé, plus l'analyse « descend » dans les différents niveaux d'imbrication.

L'option **Stockage des journaux** permet de définir le nombre maximum de journaux à stocker dans la section **Journaux d'analyse** 5.

Vous pouvez indiquer une **action par défaut** qui sera exécutée automatiquement en cas de détection de fichiers infectés. Vous pouvez choisir parmi les options suivantes :

- **Ignorer** - Aucune action n'est effectuée sur le fichier infecté (cette option n'est pas recommandée).
- **Supprimer** - Le fichier infecté est supprimé.
- **Quarantaine** (option par défaut) - Le fichier infecté est placé en **quarantaine** 5.

Les paramètres **Extensions** répertorient les types de fichiers les plus courants qui sont les plus exposés aux infiltrations sur la plateforme Android. Sélectionnez les types de fichiers à analyser ou désélectionnez les extensions à exclure de l'analyse. Ces paramètres s'appliquent à l'analyse à la demande et à l'analyse en temps réel :

- **Sensible aux extensions** - Si vous désélectionnez cette option, tous les types de fichiers sont analysés. Les fichiers sont également vérifiés, car ils sont parfois « déguisés » sous la forme d'un autre type de fichier. Dans ce cas, l'analyse est plus longue.
- **DEX (fichier du code applicatif)** - Format de fichier exécutable contenant le code compilé écrit pour le système d'exploitation Android.
- **SO (bibliothèques)** - Bibliothèques partagées et enregistrées dans les emplacements indiqués du système de fichiers et liées par des programmes qui les utilisent.
- **Archives (fichiers compressés)** - Fichiers compressés (fichiers zip).
- **Autres** - Autres types de fichiers connus.

Dans les paramètres **En temps réel**, vous pouvez configurer les paramètres de l'analyse à l'accès. L'analyse à l'accès vérifie en temps réel les fichiers que vous manipulez. Elle vérifie automatiquement le dossier des *éléments téléchargés* sur la carte SD, les fichiers d'installation *.apk*, ainsi que les fichiers de la carte SD après son montage (si l'option **Analyser les cartes SD montées** est activée). L'analyse à l'accès est lancée automatiquement au démarrage du système.

- **Protection en temps réel** - Si cette option est activée (par défaut), l'analyse à l'accès s'exécute en arrière-plan.
- **Boîte de dialogue Afficher les alertes** - Affiche des notifications d'alerte chaque fois qu'une nouvelle menace est détectée par l'analyse à l'accès.
- **Analyser les cartes SD montées** - Analyse les fichiers avant de les ouvrir ou de les enregistrer sur la carte SD.
- **Protection proactive** - Sélectionnez cette option pour appliquer les techniques d'analyse heuristique. L'analyse heuristique identifie de manière proactive les nouveaux logiciels malveillants que la version actuelle de la base des signatures de virus ne détecte pas encore : elle analyse le code et reconnaît le comportement typique des virus. Si la protection proactive est activée, l'analyse est plus longue.
- **Profondeur d'analyse des archives** - Cette option permet d'indiquer le nombre de niveaux d'imbrication des archives (fichiers *.zip*) à analyser. Plus le nombre est élevé, plus l'analyse « descend » dans les différents niveaux d'imbrication.

- **Action par défaut** - Vous pouvez indiquer une action par défaut qui sera exécutée automatiquement en cas de détection de fichiers infectés lors de l'analyse à l'accès. Si vous sélectionnez **Ignorer**, aucune action n'est effectuée sur le fichier infecté (cette option n'est pas recommandée). Si vous sélectionnez **Supprimer**, le fichier infecté est supprimé. Si vous sélectionnez **Quarantaine**, le fichier infecté est placé en **quarantaine** 5.

L'icône de notification ESET Mobile Security est affichée dans l'angle supérieur gauche de l'écran (barre d'état Android). Si vous ne souhaitez pas que cette icône apparaisse, affichez l'écran principal d'ESET Mobile Security, appuyez sur le bouton **MENU** et sur **Notifications**, puis désélectionnez l'option **Afficher l'icône**. Veuillez noter qu'en cas de risque de sécurité (analyse antivirus en temps réel désactivée, correspondance SIM désactivée, etc.), l'icône rouge d'avertissement avec point d'exclamation continue à s'afficher.

4. Antispam

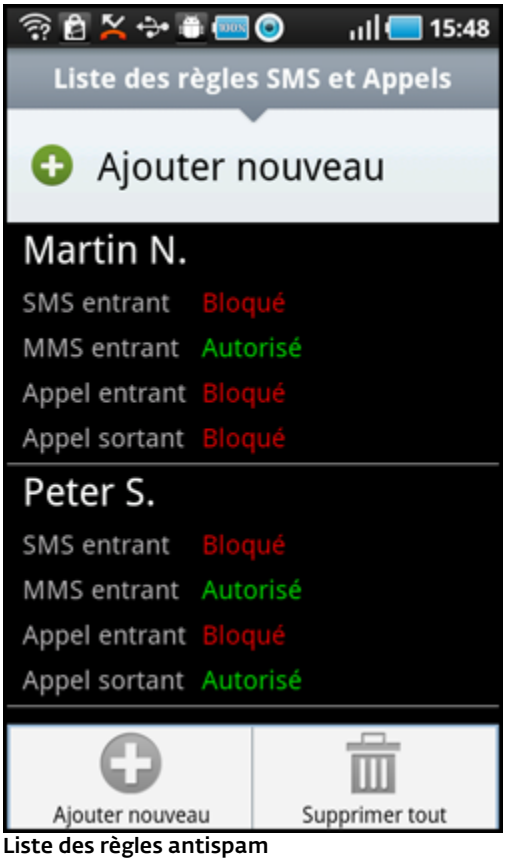
Le module **Antispam** bloque les SMS/MMS entrants, ainsi que les appels entrants/sortants en fonction des règles que vous déterminez.

Les messages non sollicités concernent habituellement des annonces de prestataires de service de téléphone portable, ou des messages d'inconnus ou d'utilisateurs non spécifiés. L'expression *blocage de message* fait référence au placement automatique d'un message entrant dans la section **Journaux de courrier indésirable** 7. Aucune notification n'est affichée lorsqu'un message entrant est bloqué. Avec cette fonction, vous n'êtes pas dérangé par des informations non sollicitées, mais vous avez toujours la possibilité de consulter la liste des messages bloqués afin de vous assurer qu'aucun message n'a été bloqué par erreur.

Pour ajouter une nouvelle règle antispam, touchez les options **Liste des règles SMS et Appels** > **Ajouter nouveau**. Saisissez le numéro de téléphone que vous souhaitez bloquer ou appuyez sur le bouton **+** pour le sélectionner dans la liste des contacts. Personnalisez la règle en autorisant ou bloquant les messages et appels, puis appuyez sur **OK**.

Pour modifier ou supprimer une entrée de règle existante, appuyez de manière prolongée sur l'entrée et choisissez l'option souhaitée dans la liste qui apparaît. Si vous souhaitez supprimer toutes les règles antispam, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

REMARQUE : le numéro de téléphone doit inclure l'indicatif international, suivi du numéro proprement dit (par exemple +16101001OO).



Liste des règles antispam

Paramètres

Bloquer les appels anonymes - Activez cette option si vous souhaitez bloquer les appelants dont le numéro de téléphone a volontairement été masqué par l'intermédiaire de la fonction de refus de présentation de la ligne appelante (CLIR ou Calling Line Identification Restriction).

Bloquer les contacts connus - Utilisez cette option pour bloquer les messages et les appels des contacts figurant dans votre liste de contacts.

Bloquer les contacts inconnus - Cette option bloque les messages et les appels des personnes ne figurant pas dans votre liste de contacts. Vous pouvez utiliser cette option pour bloquer les appels indésirables ou pour empêcher vos enfants de composer des numéros inconnus. (Il est recommandé de protéger les paramètres antispam par un **mot de passe** 10.)

Dans la section **Journaux de courrier indésirable**, vous pouvez afficher les appels et messages bloqués par le module de blocage du courrier indésirable. Chaque journal contient le nom de l'événement, le numéro de téléphone correspondant, ainsi que la date et l'heure de l'événement. Les SMS bloqués contiennent également le corps du message.

5. Anti-vol

La fonctionnalité **Anti-vol** protège votre téléphone mobile de tout accès non autorisé.

Si vous perdez votre téléphone, ou si quelqu'un le vole et remplace votre carte SIM par une autre carte (non fiable), le téléphone est verrouillé automatiquement par ESET Mobile Security. Un SMS d'alerte est envoyé secrètement aux numéros de téléphone indiqués par l'utilisateur. Ce message indique le numéro de la carte SIM insérée dans l'appareil, le numéro IMSI (numéro d'identité internationale d'abonné mobile), ainsi que le numéro IMEI (numéro d'identité internationale d'équipement mobile) de l'appareil mobile. L'utilisateur non autorisé n'a pas conscience que ce message a été envoyé puisqu'il est supprimé automatiquement des fils des **messages**. En outre, vous pouvez également demander les coordonnées GPS du téléphone qui a été perdu ou effacer à distance toutes les données stockées sur le téléphone.

Cartes SIM de confiance

Si la carte SIM qui est insérée dans votre appareil mobile est celle que vous souhaitez enregistrer comme étant fiable, appuyez sur **Ajouter**. Si vous utilisez plusieurs cartes SIM, vous souhaiterez peut-être les différencier en modifiant l'**alias de la carte SIM** (en indiquant par exemple *Bureau* ou *Maison*).

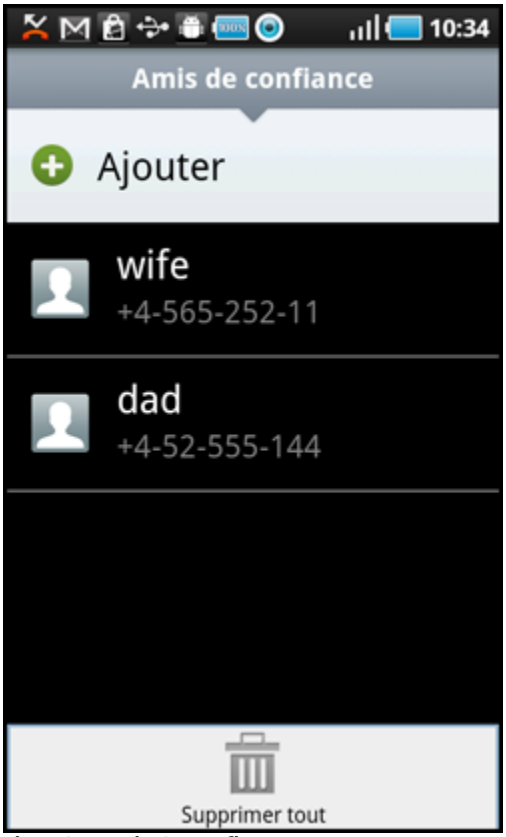
Pour **modifier** ou **supprimer** une entrée de carte SIM existante, appuyez de manière prolongée sur l'entrée et choisissez l'option souhaitée dans la liste qui apparaît. Si vous souhaitez supprimer toutes les entrées de la liste, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

Amis de confiance

Dans la liste **Amis de confiance**, **ajoutez** les numéros de téléphone qui recevront le SMS d'alerte si une carte SIM non fiable est insérée dans votre appareil. Saisissez un nom dans le champ **Nom de l'ami** et le numéro de téléphone dans le champ **Numéro de téléphone**, ou appuyez sur le bouton **+** pour sélectionner un contact dans la liste des contacts. Si le contact comporte plusieurs numéros de téléphone, le SMS d'alerte est envoyé à tous ces numéros.

Pour **modifier** ou **supprimer** une entrée existante, appuyez de manière prolongée sur l'entrée et choisissez l'option souhaitée dans la liste qui apparaît. Si vous souhaitez supprimer toutes les entrées de la liste, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

REMARQUE : le numéro de téléphone doit inclure l'indicatif international, suivi du numéro proprement dit (par exemple +161010O10O).



Liste des amis de confiance

Paramètres

Si votre appareil ne comporte pas de carte SIM (c'est le cas notamment des tablettes ou des téléphones CDMA), sélectionnez l'option **Ignorer la mise en correspondance SIM**. Ces avertissements *Risque de sécurité* affichés en rouge (concernant la *désactivation de la mise en correspondance SIM* et l'*absence de définition d'une carte SIM fiable*) sont désactivés dans l'écran principalESET Mobile Security. (Veuillez noter que l'option Ignorer la mise en correspondance SIM est désactivée sur les appareils CDMA.)

Pour activer la vérification automatique de la carte SIM insérée dans l'appareil (et l'envoi d'un SMS d'alerte), sélectionnez l'option **Activer la correspondance SIM**.

Dans le champ **Texte de l'alerte SMS**, vous pouvez modifier le message qui sera envoyé au(x) numéro(s) prédéfini(s) si une carte SIM non fiable est insérée dans votre appareil. Si vous avez acheté ESET Mobile Security sur Google Play, une adresse de messagerie de votre compte Google est insérée automatiquement. Vous pouvez également entrer une autre adresse de messagerie ou un autre numéro de contact.

Commandes SMS

Les commandes à distance SMS (« wipe », « lock » et « find ») ne fonctionnent que si l'option **Activer les commandes par SMS** est sélectionnée.

L'option **Activer la réinitialisation du mot de passe par SMS** vous permet de réinitialiser votre mot de

passe de sécurité en envoyant à votre appareil mobile un SMS depuis un appareil que vous avez enregistré dans la liste **Amis de confiance**. Ce SMS doit avoir la forme suivante :
eset remote reset

Si vous avez perdu votre appareil et souhaitez le verrouiller, envoyez à votre numéro un SMS de verrouillage à distance depuis un appareil mobile. Le SMS doit avoir le format suivant :
eset lock mot_de_passe
Remplacez *mot_de_passe* par le mot de passe que vous avez défini dans la section **Mot de passe** 10. Un utilisateur non autorisé ne pourra pas utiliser votre téléphone, car il devra entrer votre mot de passe.

Si vous souhaitez demander les coordonnées GPS de votre appareil mobile, envoyez un SMS de recherche à distance à votre numéro d'appareil mobile ou au numéro d'un utilisateur non autorisé (selon que la carte SIM a déjà été remplacée ou non) :
eset find mot_de_passe
Vous allez recevoir un SMS indiquant les coordonnées GPS et un lien vers Google Maps qui vous permettra de localiser avec précision votre appareil mobile. Veuillez noter que, pour recevoir les coordonnées GPS, vous devez activer au préalable le module GPS sur votre appareil.

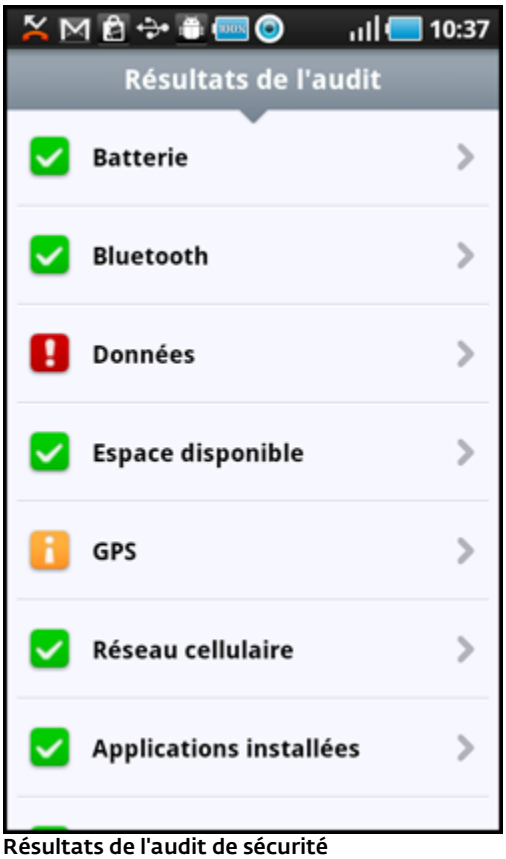
Si vous souhaitez effacer toutes les données stockées sur votre appareil et sur tous les supports amovibles qui y sont insérés, envoyez un SMS de suppression à distance :
eset wipe mot_de_passe
Tous les contacts, SMS, messages électroniques, applications installées, ainsi que votre compte Google et le contenu de la carte SIM, sont effacés de manière permanente de votre appareil. Si ESET Mobile Security n'est pas défini comme Administrateur de l'appareil, seuls les contacts, les messages et le contenu de la carte SD sont effacés.

REMARQUE : le mot de passe fait la différence entre les majuscules et les minuscules. Veillez par conséquent à le saisir exactement comme vous l'avez défini dans la section Mot de passe.

6. Audit de sécurité

L'**Audit de sécurité** vérifie différentes données concernant le téléphone : niveau de la batterie, statut Bluetooth, espace disque libre, etc.

Pour exécuter un audit de sécurité manuellement, appuyez sur **Audit**. Un rapport détaillé apparaît.



Résultats de l'audit de sécurité

La coche verte située à côté de chaque élément indique que la valeur est au-dessus de la limite ou que l'élément ne représente pas un risque de sécurité.

L'icône orange indique que la valeur d'un des éléments est au-dessous de la limite ou que l'élément pourrait représenter un risque de sécurité potentiel. Appuyez sur l'élément pour afficher les résultats détaillés.

Le point d'exclamation rouge indique que l'élément est au-dessous de la limite ou qu'il représente un risque de sécurité qui doit être résolu.

Si vous souhaitez résoudre l'état de l'élément en rouge, appuyez sur l'élément et confirmez en appuyant sur **Oui**.

Paramètres

L'audit de sécurité est planifié pour s'exécuter par défaut toutes les 24 heures. Si vous souhaitez désactiver l'audit périodique, désélectionnez l'option **Audit périodique**.

Si l'option **Correction automatique** est activée, ESET Mobile Security essaie automatiquement de corriger les éléments présentant un risque (par exemple le statut bluetooth) sans intervention de l'utilisateur. Cette option ne s'applique qu'à l'audit automatique (planifié).

L'option **Stockage des journaux** permet de définir le nombre maximum de journaux à stocker dans la section **Journaux d'audit**.

L'option **Période d'audit** permet de définir la fréquence de l'audit automatique (planifié).

Pour modifier la limite à partir de laquelle l'espace disque disponible et le niveau de batterie sont considérés comme étant faibles, utilisez les options **Limite d'espace libre du disque** et **Limite du niveau de batterie**.

Dans l'onglet **Éléments à vérifier**, sélectionnez les éléments à vérifier au cours de l'audit périodique (planifié).

La section **Journaux d'audit** contient des journaux qui fournissent des informations complètes sur les audits périodiques et déclenchés manuellement. Chaque journal contient la date et l'heure de l'événement, ainsi que les résultats détaillés de chaque élément.

Le **Gestionnaire de tâches** présente tous les processus, services et tâches qui sont exécutés sur votre appareil. ESET Mobile Security permet d'arrêter les processus, services et tâches qui ne sont pas exécutés par le système. Ils sont indiqués par une icône rouge (**x**).

7. Mise à jour

Par défaut, ESET Mobile Security est installé avec une tâche qui garantit la mise à jour régulière du programme. Pour exécuter la mise à jour manuellement, appuyez sur **Mettre à jour maintenant** .

Paramètres

L'option **Mise à jour automatique** permet de définir l'intervalle de téléchargement automatique des mises à jour des signatures de virus.

REMARQUE : afin d'éviter toute utilisation superflue de la bande passante, les mises à jour sont publiées uniquement lorsque c'est nécessaire, c'est-à-dire lorsqu'une nouvelle menace est ajoutée. Les mises à jour sont gratuites avec votre licence active, mais votre opérateur de téléphonie mobile peut facturer le transfert des données.

8. Mot de passe

Votre mot de passe de sécurité protège les paramètres de toute modification non autorisée. Le mot de passe est nécessaire dans les cas suivants :

- Accès aux fonctionnalités protégées par mot de passe d'ESET Mobile Security (Antivirus, Antispam, Anti-vol et Audit de sécurité)
- Accès à votre téléphone s'il a été verrouillé
- Envoi à votre appareil de commandes SMS
- Désinstallation d'ESET Mobile Security

REMARQUE : la désinstallation de la protection est disponible uniquement sur Android 2.2 et les versions ultérieures.

Pour définir un nouveau mot de passe de sécurité, saisissez-le dans les champs **Mot de passe** et **Ressaisissez MdP**. L'option **Phrase de rappel** (si elle est définie) affiche une astuce qui vous permet de vous remémorer votre mot de passe si vous l'avez oublié.

IMPORTANT : choisissez votre mot de passe avec soin, car vous devrez le fournir si vous souhaitez déverrouiller votre appareil mobile ou désinstaller ESET Mobile Security.

Dans l'onglet **Appliquer à**, vous pouvez indiquer les modules qui seront protégés par le mot de passe.

Si vous avez oublié votre mot de passe, vous pouvez envoyer à votre appareil mobile un SMS depuis le numéro d'un téléphone mobile enregistré dans la liste **Amis de confiance**. Ce SMS doit avoir la forme suivante :
eset remote reset
Votre mot de passe sera réinitialisé.

9. Dépannage et assistance

9.1 Dépannage

ESET Mobile Security offre une fonctionnalité de journalisation avancée qui contribue au diagnostic des problèmes techniques potentiels. Avant de contacter le service client d'ESET, il est fortement recommandé de rechercher une solution possible dans la base de connaissances ESET. Si vous devez toujours contacter le service client d'ESET, procédez comme suit :

1. Rendez-vous dans l'écran principal de ESET Mobile Security, appuyez sur le bouton **MENU** et sélectionnez **Paramètres de journalisation**.
2. Sélectionnez un composant du programme auquel le problème est lié.
3. Répliquez le problème. Des informations seront consignées dans un fichier journal de l'application.
4. Rendez-vous dans l'écran principal de ESET Mobile Security, appuyez sur le bouton **MENU** et sélectionnez **Service client**.
5. Si vous n'avez pas trouvé de solution dans notre base de connaissances, appuyez sur **Continuer**.
6. Remplissez tous les détails et appuyez sur **Soumettre** au bas de l'écran. Assurez-vous que l'option **Journal de l'application** est sélectionnée (par défaut).

9.2 Assistance technique

Pour toute assistance administrative ou technique concernant ESET Mobile Security ou tout autre produit de sécurité ESET, les experts de notre service client sont là pour vous aider.

Pour trouver des réponses aux questions les plus fréquentes, accédez à la base de connaissances ESET : *http://kb.eset.com/android*

La base de connaissances contient un grand nombre d'informations utiles qui permettent de résoudre les problèmes les plus courants. Elle est organisée en catégories et propose une fonction de recherche avancée.

Pour contacter le service client ESET, utilisez le formulaire de demande d'assistance disponible à cette adresse : *http://support.athena-gs.fr/demande_de_support.php?editeur=eset*

Pour envoyer une demande d'assistance directement à partir de votre téléphone mobile, accédez à l'écran principal ESET Mobile Security, puis appuyez sur le bouton **MENU** et sur **Service client**. Remplissez tous les champs obligatoires. Pour inclure **Journal de l'application** complet, suivez la procédure décrite dans la section Dépannage 11.